AES Candidate DEAL

Richard Outerbridge
Interac Association

August 21, 1998

Introduction

- DEA with Larger blocks
- Background & Overview
- Operation & Key Scheduling
- Speed (or lack thereof)
- Strengths & Weaknesses
- Why Bother?

Background

- All credit and almost no blame goes to...
  - DEAL designed by Lars R. Knudsen
  - Presented in Ottawa at SAC'97
- What's my interest?
  - Interac Association
  - Sometime DES programmer
  - Natural extension of DES

Overview

- The Bad News :
  - DEAL is based on the DES
  - No faster than triple-DES
- The Good News :
  - Simple, straightforward, easy
  - Better than triple-DES
- Evolutionary, not revolutionary

Operation

- No diagrams required!
- Think of the DES, with DES used as the round function
- 128-bit blocks, and 64-bit half-blocks
- For 128- & 192-bit keys, six rounds
- For 256-bit keys, eight rounds

Operational Subtleties

- Compared to the DES :
  - Left-half-block works on right
  - Final half-blocks NOT “unswapped”
    - Denies “room to play” when chaining
      - Reduced number of rounds could be exploited
    - Encryption and decryption not the same
      - Decryption must “pre-swap” and “post-swap”

Key Scheduling

- Given {2, 3, 4} 64-bit keys :
- Replicate to {6, 6, 8} 64-bit blocks
- XOR a different (1-bit) constant onto each replicated copy
- CBC encrypt the lot using DES, an IVZ of zero, and a fixed key-scheduling key
- KS key is 0x0123456789abcdef

Key Scheduling Niceties

- Endedness matters!
  - Replicant constants are:
    - <1> = 0x8000000000000000
    - <2> = 0x4000000000000000
    - <4> = 0x2000000000000000
    - <8> = 0x1000000000000000 (128 & 256)

Speed (or lack thereof)

- For 128- & 192-bit keys, just as fast (slow) as 3DES
- For 256-bit keys, and 8 rounds, only 75% as fast as 3DES
- Key scheduling very, very, slow
  - 128/192 : 6E+7K (6K?); 256 : 8E+9K (8K?)
- Reported K/S speeds : “raw DES” K/S cycles only 63% of actual

Claimed Strength

- 128-bit keys : exhaustive search
- 192-bit keys : (a) $2^{\sim 121}$ DES encryptions, 2^{70} chosen-plaintexts, 2^{64} words
- 192-bit keys : (b) $2^{\sim 168}$ DES encryptions, meet-in-the-middle attack
- 256-bit keys : $2^{\sim 224}$ DES encryptions, meet-in-the-middle attack

As Lucks Would Have It...

- *New* attacks due to Stefan Lucks, August 15, 1998 (see the BCL)
- 128-bit keys : $2^{\sim 121}$ DES encryptions, requiring 2^{70} chosen-ciphertexts
- 192-bit keys : $2^{\sim 136}$ DES encryptions, requiring 2^{70} chosen-ciphertexts
- 192-bit keys : $2^{\sim 161}$ DES encryptions, requiring 2^{48} chosen-ciphertexts

Required Strength

- "Minimal Key Lengths for Symmetric Ciphers…" (January 1996) : 76 bits
- 121-80 : 41-bit cushion, 60 years
- 136-80 : 56-bit cushion, 84 years
- 224-80 : 132-bit cushion, 216 years
- DEAL is sub-optimal, but sufficient

Unexplored Extension

- What happens if the key-scheduling key is allowed to vary?
- Another 56-bit crypto-variable?
- OR one or more classes of bad things :
  - Equivalent keys
  - Complementary keys
  - Weak keys

Weaknesses

- Based on DES
  - Breakthrough on DES breaks DEAL
- If DES has trap doors, so does DEAL
- Probably not useful for hashing
- Not well suited for dynamic rekeying
- No faster than triple-DES
- “Certificational” weaknesses

So : Why Bother?

- Better the devil you know...
  - DES already extensively studied
  - DES already extensively deployed
- Evolutionary change, using familiar technology, over the long term
  - Lower cost to implement and deploy
  - No algorithm will ever be fast enough

What, me worry?

- Were speed of adoption suddenly more critical than speed of operation...
  - "Overnight" implementation possible
  - Less worrisome when 3DES standardized
- Software is a poor excuse for hardware
  - Hardware can alway$ be fa$t enough
- Prima-facie better than 3DES
  - DEAL is an "null-hypothesis" candidate

Questions?